ETSI TS 103 307 V1.1.1 (2016-04)

CYBER;
Security Aspects for LI and RD Interfaces

Reference
DTS/CYBER-0005

Keywords
cyber security, lawful interception, retained data

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights 4
Foreword 4
Modal verbs terminology 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definitions and abbreviations 5
3.1 Definitions 5
3.2 Abbreviations 6
4 Structure of document and list of relevant interfaces 6
4.1 Introduction 6
4.2 List of LI and RD items covered in the present document 6
5 Common techniques 6
5.1 Introduction 6
5.2 Hash algorithms 7
Annex A (normative): Providing assurance for LI or RD material as evidence 8
A.1 Statement of problem 8
A.2 Techniques for providing assurance for LI or RD material as evidence 8
A.2.1 Approaches to providing assurance 8
A.2.2 Definition of two techniques 9
A.3 Detailed definition for hash-only technique in the context of Retained Data 9
A.3.1 Summary 9
A.3.2 Terminology used in clause A.3 9
A.3.3 Processes and testing 10
A.3.3.1 Process at CSP 10
A.3.3.2 Process at any LEA systems handling the Evidence Data 10
A.3.3.3 Process for use in court 10
A.3.3.4 Recommended testing and assurance process at LEA Receiver 10
A.3.4 Choice of hashing algorithms 11
A.3.5 Meta-data required 11
A.3.6 Associating hashes with the Evidence Data 11
A.3.7 Storing information at the CSP 12
A.3.8 Other notes 12
History 13

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies security processes and techniques for LI and RD systems.

The present document is limited to the provision of evidential assurance of RD material.

Future versions of the present document will cover:

1) Assurance of the integrity and originator of approvals/authorizations.

2) Security aspects of internal interfaces for Lawful Interception.

3) Security issues around the role for global, trusted-third-party or virtualised components of Law Enforcement equipment: Monitoring or Mediation facilities.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] FIPS Publication 180-4 (2014): "Secure Hash Standard (SHS)".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 102 657: "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".

[i.2] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

[i.3] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (AsiC)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 102 657 [i.1] apply.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CSP	Communications Service Provider
LI	Lawful Interception
PDF	Portable Document Format
RD	Retained Data
SHA	Secure Hash Algorithm

4 Structure of document and list of relevant interfaces

4.1 Introduction

The present document considers the list of particular information flows and interfaces for RD and LI specified in clause 4.2. It examines them from a security (confidentiality, integrity and authenticity) perspective and specifies implementation details (technologies, algorithms, options, minimum requirements on keys, etc.).

An underlying reference model for LI is given in ETSI TS 102 232-1 [i.2] and an underlying reference model for RD is given in ETSI TS 102 657 [i.1].

Certain techniques are applicable to more than one information flow or interface. Generic techniques are addressed in clause 5.

For each information flow or interface, the present document contains the following information (where applicable):

- Statement of the problem, including reference model.
- Identification of the threats and risks to the extent it is appropriate to publish in a standard.
- Statement of the techniques which are recommended as a solution.

4.2 List of LI and RD items covered in the present document

The present document addresses the following LI and RD items:

1) Providing evidential assurance of LI or RD material (Annex A).

The following topics will be covered in future versions of the present document:

1) Assurance of the integrity and originator of approvals/authorizations.
2) Security aspects of internal interfaces for Lawful Interception.
3) Security issues around the role for global, trusted-third-party or virtualised components of Law Enforcement equipment: Monitoring or Mediation facilities.

5 Common techniques

5.1 Introduction

The following techniques are used in a number of the annexes of the present document:

- Algorithms for hashing data.

The following techniques will be included in future versions of the present document:

- Digital signature algorithms.
- Procedures for Trusted timestamp.
- Transport-layer security

5.2 Hash algorithms

The SHA-256 algorithm shall be as defined in FIPS Publication 180-4 [1].

The SHA-512 algorithm shall be as defined in FIPS Publication 180-4 [1].

Annex A (normative): Providing assurance for LI or RD material as evidence

A.1 Statement of problem

The requirement is to provide assurance about the integrity of the LI or RD material (i.e. to help with assurance that it has not been altered during the course of delivery and/or storage with end user authorities) and to provide assurance about the originator of the material (i.e. the organization that produced it). The present document does not look at any requirement for confidentiality in this annex.

The goal of this clause is to add assurance to LI or RD material if it is presented as evidence in court. The present document does not attempt to examine legal aspects and no assurance is given that the process in the present document provides a complete or adequate level of assurance for any particular jurisdiction.

The reference model for this clause consists of two parties:

- The originator: the party that creates the material and wishes to provide assurance about its integrity and origin.
- The receiver: the party that wishes to check the integrity and originator of the material.

In a typical situation:

- The originator is the CSP, and the information flow starts at the point where material is selected by the CSP for use as RD or LI. The present document does not examine the integrity of existing CSP business records.
- The receiver is wherever there is a requirement to check the integrity and origin. This can include: immediately upon receiving the material at a government/police agency, or as a check by police or prosecution teams prior to court, or for checking at any time during court proceedings.

The information contained within the flow is not defined within the present document, except where it is noted that parameters (such as identifiers or timestamps) would be needed in order to meet the requirements.

A.2 Techniques for providing assurance for LI or RD material as evidence

A.2.1 Approaches to providing assurance

There is a wide range of jurisdictions in which LI/RD material is used in evidence. There is a wide range of approaches to providing assurance to LI/RD material. Specifically approaches can be broadly categorized as:

- Process-based: Some countries/jurisdictions use an approach based on demonstrating that the processes followed were in accordance with approved procedures.

EXAMPLE 1: Use a published procedure for how a Retained Data response file is stored, and demonstrate that these procedures had been followed.

- Cryptography-based: Some countries/jurisdictions use an approach based on cryptographic assurance of the integrity and origin of material.

EXAMPLE 2: If material is signed using a private key which has been stored securely, there is cryptographic assurance that it was produced by the owner of the private key.

Many countries/jurisdictions use a mix of both process-based assurance and cryptographic assurance.

The present document does not state that one approach is fundamentally better than the other. It is national choice whether to use a process-based approach or a cryptographic approach, or a mixture of the two. The present document provides a "toolkit" of cryptographic techniques which can be used. The present document describes the requirements and assurance that each technique could potentially fulfil. A threat analysis should be performed on a national basis to determine the overall mixture of techniques required. It is important that systems are designed to avoid a "bid-down" attack where techniques can be selected which are not appropriate for the threats they are trying to mitigate.

The following approaches are all examples of appropriate ways to provide evidential assurance (clearly the level of assurance provided will depend on the details used and the requirements that need to be met within the given legislation):

1) Fully process-based approach. Material is handled in accordance with a well-documented process, and appropriate records are kept to demonstrate that the process was followed and those involved were appropriately trained. This approach is not addressed further in the present document.

2) Use of hashes to add evidential assurance. Some assurance requirements can be met by the use of hashes, though others requirements (around the origin of material) would be handled separately, including the storage of the hashes securely at the originator.

3) Use of hashes and signatures to add evidential weight. This can provide assurance of the integrity and origin of the material and relies on the cryptographic material being stored securely.

This list is not exhaustive. It may be decided to start with elements of approach 1 and (where required) to move through approach 2 and eventually on to step 3 of the above list, though this progression is not essential.

A.2.2 Definition of two techniques

The following two techniques match the descriptions from the list in the clause A.2.1.

- "Hash-only technique": An example of item 2 in the list in clause A.2.1 is to use hashes to give assurance to Retained Data records. Details are given below (clause A.3) for use of the hash-only technique. Specific details for how to integrate this approach into an existing RD delivery technique are given in ETSI TS 102 657 [i.1].

- "Digital-signature technique": An example of item 3 in the list in clause A.2.2 is to use hashes and signatures to give assurance to LI information. Details for how to use this technique are given in ETSI TS 102 232-1 [i.2].

A.3 Detailed definition for hash-only technique in the context of Retained Data

A.3.1 Summary

This clause defines a technique based on hashing without using signatures. The present document describes this technique in the context of assuring the integrity of Retained Data records from the point when a request is answered by the CSP onwards (e.g. through to its use in court). However, it can be used in other contexts e.g. for material other than Retained Data or for assuring Retained Data at other stages.

This clause highlights how the present document can be used in conjunction with ETSI TS 102 657 [i.1].

A.3.2 Terminology used in clause A.3

The terms "Request" and "Response" are defined in ETSI TS 102 657 [i.1].

The "Evidence Data" is the response generated by the CSP which is required to be assured for use in evidence. The Evidence Data is considered to be immutable or "atomic" i.e. it is not possible to discard part of the evidence and assure the remainder. If information has sub-components that can be used independently then each component is considered to be a single piece of Evidence Data and is hashed separately. Clause A.3.6 details how the Evidence Data and hashes can be associated.